TITLE: Comments – NBP Public Notice #21
Docket: GN Docket Nos. 09-47, 09-51, and 09-137
Submit to: http://www.fcc.gov/cgb/ecfs/
Deadline: Wednesday December 9, 2009

Contributors
Organization: OpenID Foundation — www.openid.net

1. Brian Kissel; Chairman, OpenID Foundation; CEO, JanRain (bkissel@janrain.com)
2. Brady Brim-DeForest, OpenID Foundation Member
3. Don Thibeau, Executive Director OpenID Foundation
4. Chris Messina, OpenID Foundation community board member; CEO, Citizen Agency

Comments from the FCC
"In the course of compiling the record for the Commission's development of the National Broadband Plan,1 the Commission has invited comment on "how digital technologies ... can improve civic engagement, government at all levels, and the lives and welfare of residents and businesses." The Commission now seeks tailored comment on broadband and portability of data and their relation to cloud computing, transparency, identity, and privacy. We strongly encourage parties to develop responses to this Notice that adhere to the organization and structure of the questions in this Notice."

Resources:
http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-09-2433A1.pdf
http://blog.broadband.gov/?entryId=16259

----

1. **Government data transparency.** Data transparency refers to making data public and easily accessible over the Internet. There are many pieces of legislation requiring the publication of Federal government information. This legislation typically requires the publication of data on an agency's website. One recent initiative seeks to establish a central repository of government data. We seek comment on the potential benefits and pitfalls of increased data transparency.

a. What efficiencies can be gained through easing accessibility to public government information?

> As Vivek Kundra, the federal CIO, has mentioned in many public forums including the recent Government 2.0 Conference, a priority of the federal government is transparency and citizen engagement. By allowing citizens to access data and interact more easily across all the federal government websites, government agencies, legislators, and executives will have a greater understanding of the needs of their citizens, and citizens will be able to serve themselves more effectively and efficiently.

Specifically, by providing the private citizen a way to engage with the government without having to create one or more accounts strictly for use on government websites, the barrier to participation is greatly reduced. With this barrier out of the way, the focus can turn to convenience, ongoing interaction across sessions, and a higher degree of personalization that typifies most successful Web 2.0 properties.

b. Are there examples of innovative products or services provided by the private sector that rely upon the use of easily accessible government information?

One example is GPS and map-based navigation systems for vehicles. A great deal of the primary data for these applications come from government sources. There are a multitude of commercial services that utilize US census data.

Everyblock is an open source initiative that leverages government data at the city and state level to facilitate citizen-awareness of their surroundings and an understanding of their environment at the block and neighborhood levels. Everyblock synthesizes data from several agencies and does the hard work of providing a compelling user interface coupled with visualizations that help citizens consume broad amounts of information quickly and easily. While the Everyblock website is a popular destination, their iPhone application demonstrates how relevant, useful, and beautiful! mashed up government data can be!

c. Federal government data are available in many formats. In what formats should this data be made available over the Internet? How should open data standards inform policy for data transparency?

The role of standards in technology development cannot be underestimated. Standards form the basic underpinnings of interoperability between networked applications, and at base, provide a means for heterogeneous applications to *communicate* with one another.

In other words, if I speak English, but you speak Chinese, there is no *standard* by which we communicate — and therefore, there is no market of interchange between us. I would have little interest if you wanted to sell me a book in Chinese, and likewise, you would have little interest in a recording made in English. If we agree on a common language, however, we are able to communicate and exchange information — and more importantly — focus on higher order collaboration and interaction.

Computer programs are very similar, though in place of verbal language, we have data formats and APIs.

The role of the government in both settings standards and deciding on formats for the kind of interchange I've described above should not be underestimated. In terms of identifying opportunities and their common baselines, and amplifying the work of the broader web community, the government can act as convener, facilitator, and promoter.

In terms of specific recommendations, every type of content produced by the government that has any aspect of timeliness should be offered as a typical RSS or ATOM feed. These formats are widely supported by both popular feed aggregators like Google Reader and have broad support in web browsers. In some ways, these formats have become the *lingua franca* of Web 2.0, at their base allowing data interchange between countless unaffiliated vendors from Microsoft to Facebook to the smallest web shop.

It's worth pointing out that these formats are text-based, and though they may be somewhat arcane, are readable in any standard text editor, and can be parsed and read by a wide number of applications, including open source and free software. Binary formats are generally to be discouraged — especially those which require special plugins, viewers, or software licenses.

While there is of course much more to say on this topic, it is equally important the government *consume* as well as produce content in these formats. While on the one hand consuming information in these formats plays an important leadership role in showing others how it's done, it also makes good on the promise of government-as-platform, where the same effort that I expend to interoperate with a commercial vendor can be used to interoperate and transact data with the government.

In that respect, open standards based identity data services would seem to be of most value to citizens and the government. OpenID Attribute Exchange and SREG, OAuth, Portable Contacts, and Activity Streams represent the kinds of platforms that the federal government should adopt as they endeavor to establish bidirectional connectivity with citizens.

d. How does data transparency relate to application development? Are there potential efficiencies to be gained through an increase in government data transparency?

e. To what extent would increased data transparency affect intra-agency processes, intergovernmental coordination, and civic participation?

f. To what extent do existing regulations inhibit or promote government data transparency?

g. What impact do developments in data transparency have with respect to broadband deployment, adoption, and use?

h. What are the potential benefits to making data more accessible?

i. What potential pitfalls exist when increasing data transparency?

j. What privacy and confidentiality concerns might arise due to an increase in data transparency and what, if any, privacy safeguards are needed to protect against the misuse of personal information?

k. What types of personal information should be protected from disclosure?

> Individual data points that when combined can expose the unique identity of a user (i.e. a combination of birth date, zip code and gender) should be protected unless explicitly released by the user.

Cloud computing. When considering the portability of data, we also consider the processes through which data are moved. In this context, we seek comment on how to identify and understand cloud computing as a model for technology provisioning.

a. The National Institute of Standards and Technology defines cloud computing as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Does this definition accurately capture the concept of cloud computing?

b. What types of cloud computing exist (e.g., public, hybrid, and internal) and what are the legal and regulatory implications of their use?

c. Can present broadband network configurations handle a large-scale shift in bandwidth usage that a rapid adoption of cloud computing might cause?

d. How does cloud computing affect the reliability, scalability, security, and sustainability of information and data?

e. To what extent can the federal government leverage cloud solutions to improve intra-agency processes, intergovernmental coordination, and civic participation?

f. What impact do developments in cloud computing have with respect to broadband deployment, adoption, and use?

g. How can various parties leverage cloud computing to obtain economic or social efficiencies? Is it possible to quantify the efficiencies gained?

h. To what extent are consumers protected by industry self-regulation (e.g., the Cloud Computing Manifesto), and to what extent might additional protections be needed?

i. What specific privacy concerns are there with user data and cloud computing?

j. What precautions should government agencies take to prevent disclosure of personal information when providing data?

k. Is the use of cloud computing a net positive to the environment? Are there specific studies that quantify the environmental impact of cloud computing?

3. **Identity Management and Government Service Delivery.** Data held by the government may be personally sensitive or confidential. In this context, we seek comment on identity management as it relates to the provision of services where individuals either provide data to the government or access data that are personally sensitive or confidential.

a. What is the current state of identity management in the federal, state, local and Tribal government?

> At the federal level, identity management is governed NIST Special Publication 800-63-1 http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf (Draft Dec 2008) in support of the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections.

b. What is the spectrum of online identity credentialing required for access to online services from the government and non-governmental entities?

> OMB guidance, E-Authentication Guidance for Federal Agencies, [OMB M-04-04] defines four levels of authentication, Levels 1 to 4. These levels are defined in terms of the consequences of the authentication errors and misuse of credentials. Level 1 is the lowest assurance and Level 4 is the highest. The OMB guidance defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with the criteria for determining the level of E-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction.

c. What identity management technologies currently exist and what are their applications?

- **Username/Password** - http://en.wikipedia.org/wiki/Password. This is the most common approach used in private sector applications. It is well understood by most demographic segments of the population and is relatively easy to deploy. However, it has a couple of key limitations. First, it’s not practically scalable. While a given individual may be willing to manage a handful of username/passwords, it becomes increasingly difficult when individuals need to manage hundreds or even thousands of passwords. Secondly, and party as a result of the first challenge, passwords can become less secure when the same username/password is used across multiple websites (password reuse). In this scenario, a password that is compromised at the least secure site is then potentially compromised across all sites where that password has been used. Also, since this approach is decentralized, the end user would need to manually reset their password at each and every site where the password was compromised. And in many cases the end user may not even remember all the websites where the password was used.

- **OpenID** - http://www.openid.net and http://en.wikipedia.org/wiki/Openid.

  OpenID is an open standard that addresses the challenges of username/password mentioned above, by entrusting an identity provider to manage user authentication at each OpenID enabled website. Today some of the major OpenID providers include Google, Yahoo, AOL, MySpace, France Telecom, Telecom Italia, Verisign and a number of dedicated providers. A more comprehensive list of OpenID providers is available at the OpenID Foundation website at http://openid.net/get-an-openid/

  Additionally, PayPal has recently announced an OpenID Service specifically designed for federal government applications. The OpenID Foundation and InfoCard Foundation are collaborating with the GSA, NIST, OMB, NIH, HHA, and CIT to develop and deploy OpenID and InfoCard authentication across federal government websites. OpenID providers participating in the initial pilot include Google, Yahoo, AOL, Verisign, and PayPal.

  In additional to authentication, OpenID Simple Registration and Attribute Exchange extensions as well as the OpenID/OAuth hybrid allow end users to transfer, only with their explicit consent, personal information including data elements such as email address, gender, age, time zone, zip code, preferred language, nickname, etc.

  An additional advantage of OpenID is that a citizen can update their profiles and/or revoke access to websites from a central service with their identity provider. If a citizen changes their email address, their ID provider can update all the websites that are utilizing that ID service. Also, if a user wants to disable access to one, many, or all websites using the ID service, they can do that from one point of interaction, they won't have to go to each website individually to make the change.

  Finally, OpenID is entirely web-based, so end users don't need to download, install, or configure any software. That means utilization levels will be higher and support costs will be lower than approaches that may require client-side software installation.

- **InfoCard** - http://en.wikipedia.org/wiki/Infocard and http://informationcard.net/foundation
- **Security Assertion Markup Language (SAML)** - http://en.wikipedia.org/wiki/Saml

d. How have HSPD-12 implementation efforts affected the efficiency of the federal government?11

HSPD-12 has played an important role in the Open Identity Initiative and the establishment of the subsequent Trust Framework Provider Adoption Process, of which the OpenID Foundation has a draft submission under review.

e. What identity management technologies are available in the private sector? What are their applications?

f. What impact do developments in identity management, such as Open ID, have with respect to broadband deployment, adoption, and use?

OpenID is potentially well suited to facilitate and accelerate the utilization and citizen benefits of broadband deployment. As lower cost broadband services reach a higher percentage of our population, government and private sector service providers will increasingly leverage this channel to offer richer, more personalized, and more cost effective offerings to their citizens and customers respectively.

However, in order to provide the best services, citizens and customers will need to authenticate themselves for many applications to set preferences, to customize their experiences, and for more interactive transactions. As more organizations drive to engage their stakeholders through the internet, and as consumers respond by utilizing faster, better, and cheaper services over the internet, the scalability of username/password authentication will become a constraint. This is exactly the use case that OpenID was designed to address - more scalable, convenient, and secure authentication across the open internet.

g. What are the potential benefits of a coordinated nationwide identity management schema?

If you mean a government run identity management schema and/or service, we think there are very limited benefits. If you mean having the federal government adopt and deploy open standards such as OpenID and OAuth across federal websites, we think that there are many benefits.

By agreeing to adopt various identity standards, the government can help to advance the state of interoperability and the portability of identity between heterogeneous networks, increasing convenience for individual citizen-participants, and reducing complexity for service providers and organizations.

As identity acts as a core building block of the social web, the future health and competitive nature of the web requires that digital identities be as portable as phone numbers, and that users — from the citizen perspective — have viable alternatives for managing and representing their identities online.

Additionally, a universal identity system that is as robust and distributed as the internet would greatly enhance and encourage citizen engagement and participation from the lowest levels of civic administration to the highest levels of the federal government. By promoting choice through interoperability, the government can create an entirely new competitive marketplace for innovation and service, founded on a basis of open technology.

h. What are the potential pitfalls of a coordinated nationwide identity management strategy?

For a government specified and run solution, the pitfalls are single-point of failure, threats to privacy, rapid obsolescence, and security. Many segments of the population are unlikely to trust a federal government run identity management system. Additionally, a government run system is likely to cost more than an open market approach that leverages open standards such as OpenID and OAuth. Further, a government run system is unlikely to innovate and evolve at the rate of the open market, limiting the government's ability to leverage the innovations of commercial providers competing for mindshare and marketshare of end users and website operators.

i. What specific privacy concerns are there with identity management strategies?

There are always concerns about privacy, security, and anonymity when it comes to identity and digital profiles. Indeed, there have been abuses and cases where people's expectations were not met by various entrusted parties' action. However, on the whole, the next generation of digital natives demand a greater degree of functionality, access, and convenience and on the surface, appear willing to exchange some personal data for these benefits. Appropriate implementation and enforcement of terms of service (TOS) and privacy policies are critical to protecting user privacy regardless of the identity management technology.

With proper data protection, encryption, disclosure of practices, and the ability to opt-out from personalization features, many potential privacy concerns can be addressed.

Moreover to the point, providing this kind of opt-in participation model (presumably with functionally reasonable defaults) can actually increase participation, because people feel a greater sense of control and agency over the way that their data is used and accessed. In this case, transparency in how data is collected, used, and can be audited is paramount.

One of the greatest privacy concerns that seems to exist (and is not restricted to digital privacy) is how access to one's personal data is limited, or restricted, to a set of known parties. That is, if an individual provides data to someone, there is an implicit belief that that data will be protected, and not released to third parties without the owner's consent. While this is not always the case in practice, it would seem that many concerns about threats to privacy derive primary from the case where some unknown third party gains an information advantage over an individual who did not expect them to have access.

Once again, protecting and preserving privacy, and setting honest and clear expectations about the use of personal data is an effective way to increase the trust and use in a system, and should be strongly considered in the design of any federally supported identity scheme.

j. What types of personal information should be protected from disclosure?